

Notice of Allowability

Application No.

10/619,031

Examiner

Minh Dinh

Applicant(s)

CHATEAU ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the examiner's amendment authorized on 7/18/07.
2. ☒ The allowed claim(s) is/are 1,2,4,6-8,10,12-15 and 18-21.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Dolly Wu on 7/18/07.

The claims have been amended as follows:

Claim 1. (currently amended) A computing device comprising:

- a processing system;

- an externally-accessible memory coupled to the processing system;

- a secret identification number generated for the computing device and stored in a secure memory that is not externally-accessible;

- a key generator for generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;

- a symmetrical encryption system to generate an encrypted key by symmetrically encrypting the random key using the secret identification number;

- wherein the processing system associates a digital certificate with an electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number;

- wherein the random key is used to sign the file digital certificate, the electronic file is ~~optionally~~ encrypted using the random key, the electronic file is accessed when the file digital

Art Unit: 2132

certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and

the externally-accessible memory further comprising an asymmetric manufacture certificate to bind firmware to the processing system.

Claim 2. (currently amended) The computing device of claim 1 wherein digital certificate contains a software signature ~~that is symmetrically encrypted using the random key~~; wherein the software signature comprises ~~is a signature for~~ hash of the electronic file that is symmetrically encrypted using the random key.

Claim 3. (canceled)

Claim 5. (canceled)

Claim 7. (currently amended) A method of providing security to files stored in an externally-accessible memory of a computing device comprising the steps of:

storing a secret identification number for the computing device in a secure memory that is not externally-accessible;

generating a random key;

generating an encrypted_key by symmetrically encrypting the random key using the secret identification number;

associating a digital certificate with ~~the~~ an electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after restoring the random key through decryption of the encrypted key with the secret identification number;

Art Unit: 2132

using the random key to sign the file digital certificate, and ~~optionally~~ encrypting the electronic file using the random key, and wherein the electronic file is accessed when the file digital certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and

binding firmware to the computing device by an asymmetric manufacture certificate in the externally-accessible memory.

Claim 8. (currently amended) The method of claim 7 wherein the associating step includes the step of generating a software signature encrypted using the random key and storing the software signature in the digital certificate; wherein the software signature comprises ~~is a signature for hash of~~ the electronic file that is symmetrically encrypted using the random key.

Claim 9. (canceled)

Claims 16-17. (canceled)

Claim 18. (currently amended) The computing device of claim 1 ~~A device with a security system for electronic files including a platform certificate comprising:~~

- ~~—— a processing system;~~
- ~~—— an externally-accessible memory coupled to the processing system;~~
- ~~—— a secret identification number generated for the computing device and stored in a secure memory that is not externally-accessible;~~
- ~~—— a key generator for generating a random key associated with a selected electronic file to be stored in the externally-accessible memory;~~

Art Unit: 2132

~~— a symmetrical encryption system to generate an encrypted key by symmetrically encrypting the random key using the secret identification number;~~

~~— wherein the processing system associates a digital certificate with the electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number; —~~

~~— wherein the random key is used to sign the file certificate, the electronic file is optionally encrypted using the random key, the electronic file is accessed when the file certificate is verified using the random key and the encrypted electronic file is decrypted using the random key; and~~

wherein the encryption of the electronic file can be bypassed and the digital platform certificate decouples allows from modification prevention detection and authentication of the electronic file.

Claim 20. (currently amended) The computing device of claim 1 further comprising ~~A device with a security system for electronic files including a manufacturer certificate comprising:~~

~~a processor;~~

an internal permanent memory in the processing system ~~processor;~~

the internal permanent memory for storing a first manufacturer's public key, wherein the first manufacturer's public key is optionally hashed and cannot be modified after writing into permanent memory;

~~an externally-accessible memory coupled to the processor;~~

the externally-accessible memory comprises the manufacturer certificate for asymmetric encryption and for prevention of firmware modification and copying; wherein the manufacturer certificate comprises a second manufacturer's public key; and

the processor for comparing the first and second manufacturer public keys and generating a pass or fail output to indicate a match.

2. The following is an examiner's statement of reasons for allowance: the prior art fails to teach "the processing system associates a digital certificate with an electronic file, where the digital certificate contains the encrypted key, such that the electronic file can be accessed only after the processing system restores the random key through decryption of the encrypted key with the secret identification number, wherein the random key is used to sign the digital certificate, the electronic file is encrypted using the random key, the electronic file is accessed when the digital certificate is verified using the random key and the encrypted electronic file is decrypted using the random key". The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number

Application/Control Number: 10/619,031
Art Unit: 2132

Page 7


is 571-272-3802. The examiner can normally be reached on Mon-Fri:
10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

7/18/07


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100